

# VANISHING IDEALS OVER FINITE FIELDS

AZUCENA TOCHIMANI AND RAFAEL H. VILLARREAL

**ABSTRACT.** Let  $\mathbb{F}_q$  be a finite field, let  $\mathbb{X}$  be a subset of a projective space  $\mathbb{P}^{s-1}$ , over the field  $\mathbb{F}_q$ , parameterized by rational functions, and let  $I(\mathbb{X})$  be the vanishing ideal of  $\mathbb{X}$ . The main result of this paper is a formula for  $I(\mathbb{X})$  that will allow us to compute: (i) the algebraic invariants of  $I(\mathbb{X})$ , and (ii) the basic parameters of the corresponding Reed-Muller-type code.

## 1. INTRODUCTION

In this paper we study vanishing ideals of sets in projective spaces parameterized by rational functions over finite fields.

Let  $R = K[\mathbf{y}] = K[y_1, \dots, y_n]$  be a polynomial ring over a finite field  $K = \mathbb{F}_q$  and let  $F$  be a finite set  $\{f_1/g_1, \dots, f_s/g_s\}$  of rational functions in  $K(\mathbf{y})$ , the quotient field of  $R$ , where  $f_i$  (resp.  $g_i$ ) is in  $R$  (resp.  $R \setminus \{0\}$ ) for all  $i$ . As usual we denote the affine and projective spaces over the field  $K$  by  $\mathbb{A}^s$  and  $\mathbb{P}^{s-1}$ , respectively. Points of the projective space  $\mathbb{P}^{s-1}$  are denoted by  $[\alpha]$ , where  $0 \neq \alpha \in K^s$ . The *projective set parameterized*  $F$ , denoted by  $\mathbb{X}$ , is the set of all points

$$[(f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))]$$

in  $\mathbb{P}^{s-1}$  that are well defined, i.e.,  $x \in K^n$ ,  $f_i(x) \neq 0$  for some  $i$ , and  $g_i(x) \neq 0$  for all  $i$ .

Let  $S = K[t_1, \dots, t_s] = \bigoplus_{d=0}^{\infty} S_d$  be a polynomial ring over the field  $K$  with the standard grading. The graded ideal  $I(\mathbb{X})$  generated by the homogeneous polynomials of  $S$  that vanish at all points of  $\mathbb{X}$  is called the *vanishing ideal* of  $\mathbb{X}$ .

There are good reasons to study vanishing ideals over finite fields. They are used in algebraic geometry [6] and algebraic coding theory [3]. They are also used in polynomial interpolation problems [12].

We come to our main result.

**Theorem 3.8** *Let  $B = K[y_0, y_1, \dots, y_n, z, t_1, \dots, t_s]$  be a polynomial ring over  $K = \mathbb{F}_q$ . If  $\mathbb{X}$  is a projective set parameterized by rational functions  $f_1/g_1, \dots, f_s/g_s$  in  $K(\mathbf{y})$ , then*

$$I(\mathbb{X}) = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S.$$

Using the computer algebra system *Macaulay2* [4], this result can be used to compute the degree, regularity, and Hilbert polynomial of  $I(\mathbb{X})$  (see Example 3.17).

By the algebraic methods introduced in [11] (see Section 2), this result can also be used to compute the basic parameters (length, dimension, minimum distance) of the corresponding projective Reed-Muller-type code over  $\mathbb{X}$  (see Example 3.18).

For all unexplained terminology and additional information, we refer to [2, 6, 8] (for algebraic geometry and computational commutative algebra) and [13] (for coding theory).

---

2000 *Mathematics Subject Classification.* Primary 13P25; Secondary 14G50, 11T71, 94B27.

The first author was partially supported by CONACyT. The second author was partially supported by SNI.

## 2. PRELIMINARIES

All results of this section are well-known. To avoid repetitions, we continue to employ the notations and definitions used in Section 1.

If  $d \in \mathbb{N}$ , let  $S_d$  denote the set of homogeneous polynomials of degree  $d$  in  $S$ , together with the zero polynomial. Thus  $S_d$  is a  $K$ -linear space and  $S = \bigoplus_{d=0}^{\infty} S_d$ .

**Definition 2.1.** An ideal  $I \subset S$  is *graded* if  $I$  is generated by homogeneous polynomials.

**Proposition 2.2.** [10, p. 92] *Let  $I \subset S$  be an ideal. The following conditions are equivalent:*

- (g<sub>1</sub>)  *$I$  is a graded ideal.*
- (g<sub>2</sub>) *If  $f = \sum_{d=0}^r f_d$  is in  $I$ ,  $f_d \in S_d$  for  $d = 0, \dots, r$ , then each  $f_d$  is in  $I$ .*

Let  $I$  be a graded ideal of  $S$  of dimension  $k$ . As usual, by the *dimension* of  $I$  we mean the Krull dimension of  $S/I$ . The *Hilbert function* of  $S/I$  is the function  $H_I: \mathbb{N} \rightarrow \mathbb{N}$  given by

$$H_I(d) = \dim_K(S_d/I_d),$$

where  $I_d = I \cap S_d$ . There is a unique polynomial  $h_I(x) \in \mathbb{Q}[x]$  of degree  $k - 1$  such that  $h_I(d) = H_I(d)$  for  $d \gg 0$  [5, p. 330]. By convention, the zero polynomial has degree  $-1$ .

The *degree* or *multiplicity* of  $S/I$  is the positive integer

$$\deg(S/I) := \begin{cases} (k-1)! \lim_{d \rightarrow \infty} H_I(d)/d^{k-1} & \text{if } k \geq 1, \\ \dim_K(S/I) & \text{if } k = 0. \end{cases}$$

**Definition 2.3.** The *regularity* of the Hilbert function of  $S/I$ , or simply the *regularity* of  $S/I$ , denoted  $\text{reg}(S/I)$ , is the least integer  $r \geq 0$  such that  $H_I(d)$  is equal to  $h_I(d)$  for  $d \geq r$ .

We will use the following multi-index notation: for  $a = (a_1, \dots, a_s) \in \mathbb{Z}^s$ , set  $t^a = t_1^{a_1} \cdots t_s^{a_s}$ . We call  $t^a$  a *Laurent monomial*. If  $a_i \geq 0$  for all  $i$ ,  $t^a$  is a *monomial* of  $S$ . An ideal of  $S$  generated by polynomials of the form  $t^a - t^b$ , with  $a, b$  in  $\mathbb{N}^s$ , is called a *binomial ideal* of  $S$ .

**Lemma 2.4.** [14, p. 321] *Let  $B = K[y_1, \dots, y_n, t_1, \dots, t_s]$  be a polynomial ring over a field  $K$ . If  $I$  is a binomial ideal of  $B$ , then the reduced Gröbner basis of  $I$  with respect to any term order consists of binomials and  $I \cap K[t_1, \dots, t_s]$  is a binomial ideal of  $S$ .*

**Proposition 2.5.** [7, pp. 136–137] *Let  $K = \mathbb{F}_q$  be a finite field and let  $\mathbb{A}^s$  be the affine space of dimension  $s$  over  $K$ . Then  $I(\mathbb{A}^s) = (\{t_i^q - t_i\}_{i=1}^s)$ .*

**Projective Reed-Muller-type codes.** In this part we introduce the family of projective Reed-Muller-type codes and its connection to vanishing ideals and Hilbert functions.

Let  $K = \mathbb{F}_q$  be a finite field and let  $\mathbb{Y} = \{P_1, \dots, P_m\} \neq \emptyset$  be a subset of  $\mathbb{P}^{s-1}$  with  $m = |\mathbb{Y}|$ . Fix a degree  $d \geq 1$ . For each  $i$  there is  $f_i \in S_d$  such that  $f_i(P_i) \neq 0$ . There is a well-defined  $K$ -linear map:

$$(2.1) \quad \text{ev}_d: S_d = K[t_1, \dots, t_s]_d \rightarrow K^{|\mathbb{Y}|}, \quad f \mapsto \left( \frac{f(P_1)}{f_1(P_1)}, \dots, \frac{f(P_m)}{f_m(P_m)} \right).$$

The image of  $S_d$  under  $\text{ev}_d$ , denoted by  $C_{\mathbb{Y}}(d)$ , is called a *projective Reed-Muller-type code* of degree  $d$  over the set  $\mathbb{Y}$  [3]. There is an isomorphism of  $K$ -vector spaces  $S_d/I(\mathbb{Y})_d \simeq C_{\mathbb{Y}}(d)$ . It is usual to denote the Hilbert function  $S/I(\mathbb{Y})$  by  $H_{\mathbb{Y}}$ . Thus  $H_{\mathbb{Y}}(d)$  is equal to  $\dim_K C_{\mathbb{Y}}(d)$ . The *minimum distance* of the linear code  $C_{\mathbb{Y}}(d)$ , denoted  $\delta_{\mathbb{Y}}(d)$ , is given by

$$\delta_{\mathbb{Y}}(d) := \min\{\omega(v) : 0 \neq v \in C_{\mathbb{Y}}(d)\},$$

where  $\omega(v)$  is the *Hamming weight* of  $v$ , that is,  $\omega(v)$  is the number of non-zero entries of  $v$ .

**Definition 2.6.** The *basic parameters* of the linear code  $C_{\mathbb{Y}}(d)$  are: its *length*  $|\mathbb{Y}|$ , *dimension*  $\dim_K C_{\mathbb{Y}}(d)$ , and *minimum distance*  $\delta_{\mathbb{Y}}(d)$ .

The following summarizes the well-known relation between projective Reed-Muller-type codes and the theory of Hilbert functions.

**Proposition 2.7.** ([3], [11]) *The following hold.*

- (i)  $H_{\mathbb{Y}}(d) = \dim_K C_{\mathbb{Y}}(d)$  for  $d \geq 0$ .
- (ii)  $\deg(S/I(\mathbb{Y})) = |\mathbb{Y}|$ .
- (iii)  $\delta_{\mathbb{Y}}(d) = 1$  for  $d \geq \deg(S/I(\mathbb{Y}))$ .

### 3. RATIONAL PARAMETERIZATIONS OVER FINITE FIELDS

We continue to employ the notations and definitions used in Sections 1 and 2. Throughout this section  $K = \mathbb{F}_q$  is a finite field and  $\mathbb{X}$  is the projective set parameterized by the rational functions  $F = \{f_1/g_1, \dots, f_s/g_s\}$  in  $K(\mathbf{y})$ .

**Theorem 3.1.** (Combinatorial Nullstellensatz [1]) *Let  $S = K[t_1, \dots, t_s]$  be a polynomial ring over a field  $K$ , let  $f \in S$ , and let  $a = (a_i) \in \mathbb{N}^s$ . Suppose that the coefficient of  $t^a$  in  $f$  is non-zero and  $\deg(f) = a_1 + \dots + a_s$ . If  $A_1, \dots, A_s$  are subsets of  $K$ , with  $|A_i| > a_i$  for all  $i$ , then there are  $x_1 \in A_1, \dots, x_s \in A_s$  such that  $f(x_1, \dots, x_s) \neq 0$ .*

**Lemma 3.2.** *Let  $K$  be a field and let  $A_1, \dots, A_s$  be a collection of non-empty finite subsets of  $K$ . If  $Y := A_1 \times \dots \times A_s \subset \mathbb{A}^s$ ,  $g \in I(Y)$  and  $\deg_{t_i}(g) < |A_i|$  for  $i = 1, \dots, s$ , then  $g = 0$ . In particular if  $g$  is a polynomial of  $S$  that vanishes at all points of  $\mathbb{A}^s$ , then  $g = 0$ .*

*Proof.* We proceed by contradiction. Assume that  $g$  is not zero. Then, there is a monomial  $t^a = t_1^{a_1} \dots t_s^{a_s}$  of  $g$  with  $\deg(g) = a_1 + \dots + a_s$  and  $a = (a_1, \dots, a_s) \neq 0$ . As  $\deg_{t_i}(g) < |A_i|$  for all  $i$ , then  $a_i < |A_i|$  for all  $i$ . Thus, by Theorem 3.1, there are  $x_1, \dots, x_s$  with  $x_i \in A_i$  for all  $i$  such that  $g(x_1, \dots, x_s) \neq 0$ , a contradiction to the assumption that  $g$  vanishes on  $Y$ .  $\square$

**Definition 3.3.** The *affine set parameterized by  $F$* , denoted  $\mathbb{X}^*$ , is the set of all points

$$(f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))$$

in  $\mathbb{A}^s$  such that  $x \in K^n$  and  $g_i(x) \neq 0$  for all  $i$ .

**Lemma 3.4.** *Let  $K = \mathbb{F}_q$  be a finite field. The following conditions are equivalent:*

- (a)  $g_1 \dots g_s$  vanishes at all points of  $K^n$ .
- (b)  $g_1 \dots g_s \in (\{y_i^q - y_i\}_{i=1}^n)$ .
- (c)  $(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \dots g_s - 1) \cap S = S$ .
- (d)  $\mathbb{X}^* = \emptyset$ .

*Proof.* (a)  $\Leftrightarrow$  (b)): This follows at once from Proposition 2.5.

(a)  $\Leftrightarrow$  (d)): This follows from the definition of  $\mathbb{X}^*$ .

(c)  $\Rightarrow$  (a)): We can write  $1 = \sum_{i=1}^s a_i(g_i t_i - f_i z) + \sum_{j=1}^n b_j(y_j^q - y_j) + h(y_0 g_1 \dots g_s - 1)$ , where the  $a_i$ 's,  $b_j$ 's and  $h$  are polynomials in the variables  $y_j$ 's,  $t_i$ 's,  $y_0$  and  $z$ . Take an arbitrary point  $x = (x_i)$  in  $K^n$ . In the equality above, making  $y_i = x_i$  for all  $i$ ,  $z = 0$  and  $t_i = 0$  for all  $i$ , we get that  $1 = h_1(y_0 g_1(x) \dots g_s(x) - 1)$  for some  $h_1$ . If  $(g_1 \dots g_s)(x) \neq 0$ , then  $h_1(y_0 g_1(x) \dots g_s(x) - 1)$  is a polynomial in  $y_0$  of positive degree, a contradiction. Thus  $(g_1 \dots g_s)(x) = 0$ .

(b)  $\Rightarrow$  (c)): Writing  $g_1 \cdots g_s = \sum_{j=1}^n b_j(y_j^q - y_j)$ , we get  $y_0 g_1 \cdots g_s - 1 = -1 + \sum_{j=1}^n y_0 b_j(y_j^q - y_j)$ . Thus 1 is in the ideal  $(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1)$ .  $\square$

**Lemma 3.5.** *Let  $f_1/g_1, \dots, f_s/g_s$  be rational functions of  $K(\mathbf{y})$  and let  $f = f(t_1, \dots, t_s)$  be a polynomial in  $S$  of degree  $d$ . Then*

$$g_1^{d+1} \cdots g_s^{d+1} f = \sum_{i=1}^s g_1 \cdots g_s h_i(g_i t_i - f_i) + g_1^{d+1} \cdots g_s^{d+1} f(f_1/g_1, \dots, f_s/g_s)$$

for some  $h_1, \dots, h_s$  in the polynomial ring  $K[y_1, \dots, y_n, t_1, \dots, t_s]$ . If  $f$  is homogeneous and  $z$  is a new variable, then

$$g_1^{d+1} \cdots g_s^{d+1} f = \sum_{i=1}^s g_1 \cdots g_s h_i(g_i t_i - f_i z) + g_1^{d+1} \cdots g_s^{d+1} z^d f(f_1/g_1, \dots, f_s/g_s)$$

for some  $h_1, \dots, h_s$  in the polynomial ring  $K[y_1, \dots, y_n, z, t_1, \dots, t_s]$ .

*Proof.* We can write  $f = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r}$  with  $\lambda_i \in K^*$  and  $m_i \in \mathbb{N}^s$  for all  $i$ . Write  $m_i = (m_{i1}, \dots, m_{is})$  for  $1 \leq i \leq r$  and set  $I = (\{g_i t_i - f_i\}_{i=1}^s)$ . By the binomial theorem, for all  $i, j$ , we can write

$$t_j^{m_{ij}} = [(t_j - (f_j/g_j)) + (f_j/g_j)]^{m_{ij}} = (h_{ij}/g_j^{m_{ij}}) + (f_j/g_j)^{m_{ij}},$$

for some  $h_{ij} \in I$ . Hence for any  $i$  we can write

$$t^{m_i} = t_1^{m_{i1}} \cdots t_s^{m_{is}} = (G_i/g_1^{m_{i1}} \cdots g_s^{m_{is}}) + (f_1/g_1)^{m_{i1}} \cdots (f_s/g_s)^{m_{is}},$$

where  $G_i \in I$ . Notice that  $m_{i1} + \cdots + m_{is} \leq d$  for all  $i$  because  $f$  has degree  $d$ . Then substituting these expressions for  $t^{m_1}, \dots, t^{m_s}$  in  $f = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r}$  and multiplying  $f$  by  $g_1^{d+1} \cdots g_s^{d+1}$ , we obtain the required expression.

If  $f$  is homogeneous of degree  $d$ , the required expression for  $g_1^{d+1} \cdots g_s^{d+1} f$  follows from the first part by considering the rational functions  $f_1 z/g_1, \dots, f_s z/g_s$ , i.e., by replacing  $f_i$  by  $f_i z$ , and observing that  $f(f_1 z, \dots, f_s z) = z^d f(f_1, \dots, f_s)$ .  $\square$

**Lemma 3.6.** *Let  $K = \mathbb{F}_q$  be a finite field. The following conditions are equivalent:*

- (a)  $(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S = (t_1, \dots, t_s)$ .
- (b)  $\mathbb{X}^* = \{0\}$ .

*Proof.* (a)  $\Rightarrow$  (b)): By Lemma 3.4,  $\mathbb{X}^* \neq \emptyset$ . Take a point  $P$  in  $\mathbb{X}^*$ , i.e., there is  $x = (x_i) \in \mathbb{A}^s$  such that  $g_i(x) \neq 0$  for all  $i$  and  $P = (f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))$ . By hypothesis, for each  $t_k$ , we can write

$$(3.1) \quad t_k = \sum_{i=1}^s a_i(g_i t_i - f_i z) + \sum_{j=1}^n b_j(y_j^q - y_j) + h(y_0 g_1 \cdots g_s - 1),$$

where the  $a_i$ 's,  $b_j$ 's and  $h$  are polynomials in the variables  $y_j$ 's,  $t_i$ 's,  $y_0$  and  $z$ . From Eq. (3.1), making  $y_i = x_i$  for all  $i$ ,  $y_0 = 1/g_1(x) \cdots g_s(x)$ ,  $t_i = f_i(x)/g_i(x)$  for all  $i$ , and  $z = 1$ , we get that  $f_k(x)/g_k(x) = 0$ . Thus  $P = 0$ .

(b)  $\Rightarrow$  (a)): Setting  $I = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1)$ , by Lemma 3.4 one has that  $I \cap S \subsetneq S$ . Thus it suffices to show that  $t_k \in I \cap S$  for all  $k$ . Notice that  $g_1 \cdots g_s f_k$

vanishes at all points of  $\mathbb{A}^s$  because  $\mathbb{X}^* = \{0\}$ . Hence, thanks to Proposition 2.5,  $g_1 \cdots g_s f_k$  is in  $(\{y_i^q - y_i\}_{i=1}^n)$ . Setting  $w = y_0 g_1 \cdots g_s - 1$ , and applying Lemma 3.5 with  $f = t_k$ , we can write

$$(w+1)^2 t_k = \sum_{i=1}^s y_0^2 g_1 \cdots g_s h_i (g_i t_i - f_i z) + y_0^2 g_1^2 \cdots g_s^2 z (f_k / g_k).$$

Therefore  $(w+1)^2 t_k \in I$ . Thus  $t_k \in I \cap S$ .  $\square$

**Lemma 3.7.** *If  $I = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1)$  and  $\mathfrak{m} = (t_1, \dots, t_s)$  is the irrelevant maximal ideal of  $S$ , then*

- (a)  $I \cap S$  is a graded ideal of  $S$ , and
- (b)  $\mathbb{X} \neq \emptyset$  if and only if  $I \cap S \subsetneq \mathfrak{m}$ .

*Proof.* (a): We set  $B = K[y_0, y_1, \dots, y_n, z, t_1, \dots, t_s]$ . Take  $0 \neq f \in I \cap S$  and write it as  $f = f_1 + \cdots + f_r$ , where  $f_i$  is a homogeneous polynomial of degree  $d_i$  and  $d_1 < \cdots < d_r$ . By induction, using Proposition 2.2, it suffices to show that  $f_r \in I \cap S$ . We can write

$$f = \sum_{i=1}^s a_i (g_i t_i - f_i z) + \sum_{i=1}^n c_i (y_i^q - y_i) + c (y_0 g_1 \cdots g_s - 1),$$

where the  $a_i$ 's,  $c_i$ 's, and  $c$  are in  $B$ . Making the substitution  $t_i \rightarrow t_i v$ ,  $z \rightarrow z v$ , with  $v$  an extra variable, and regarding  $f(t_1 v, \dots, t_s v)$  as a polynomial in  $v$  it follows readily that  $v^{d_r} f_r$  is in the ideal generated by  $\mathcal{B} = \{g_i t_i v - f_i z v\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n \cup \{y_0 g_1 \cdots g_s - 1\}$ . Writing  $v^{d_r} f_r$  as a linear combination of  $\mathcal{B}$ , with coefficients in  $B$ , and making  $v = 1$ , we get that  $f_r \in I \cap S$ .

(b):  $\Rightarrow$  If  $\mathbb{X} \neq \emptyset$ , by Lemma 3.4, we get that  $I \cap S \neq S$ . By part (a) the ideal  $I \cap S$  is graded. Hence  $I \cap S \subsetneq \mathfrak{m}$ .

$\Leftarrow$  If  $I \cap S \subsetneq \mathfrak{m}$ , by Lemmas 3.4 and 3.6, we get  $\mathbb{X}^* \neq \emptyset$  and  $\mathbb{X}^* \neq \{0\}$ . Thus  $\mathbb{X} \neq \emptyset$ .  $\square$

We come to the main result of this paper.

**Theorem 3.8.** *Let  $B = K[y_0, y_1, \dots, y_n, z, t_1, \dots, t_s]$  be a polynomial ring over a finite field  $K = \mathbb{F}_q$ . If  $\mathbb{X}$  is a projective set parameterized by rational functions  $f_1/g_1, \dots, f_s/g_s$  in  $K(\mathbf{y})$  and  $\mathbb{X} \neq \emptyset$ , then*

$$I(\mathbb{X}) = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S.$$

*Proof.* We set  $I = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1)$ . First we show the inclusion  $I(\mathbb{X}) \subset I \cap S$ . Take a homogeneous polynomial  $f = f(t_1, \dots, t_s)$  of degree  $d$  that vanishes at all points of  $\mathbb{X}$ . Setting  $w = y_0 g_1 \cdots g_s - 1$ , by Lemma 3.5, we can write

$$(3.2) \quad (w+1)^{d+1} f = \sum_{i=1}^s y_0^{d+1} g_1 \cdots g_s a_i (g_i t_i - f_i z) + z^d y_0^{d+1} g_1^{d+1} \cdots g_s^{d+1} f(f_1/g_1, \dots, f_s/g_s),$$

where  $a_1, \dots, a_s$  are in  $B$ . We set  $H = g_1^{d+1} \cdots g_s^{d+1} f(f_1/g_1, \dots, f_s/g_s)$ . This is a polynomial in  $K[\mathbf{y}]$ . Thus, by the division algorithm in  $K[\mathbf{y}]$  (see [2, Theorem 3, p. 63]), we can write

$$(3.3) \quad H = H(y_1, \dots, y_n) = \sum_{i=1}^n h_i (y_i^q - y_i) + G(y_1, \dots, y_n)$$

for some  $h_1, \dots, h_n$  in  $K[\mathbf{y}]$ , where the monomials that occur in  $G = G(y_1, \dots, y_n)$  are not divisible by any of the monomials  $y_1^q, \dots, y_n^q$ , i.e.,  $\deg_{y_i}(G) < q$  for  $i = 1, \dots, n$ . Therefore, using

Eqs. (3.2) and (3.3), we obtain the equality

$$(3.4) \quad (w+1)^{d+1}f = \sum_{i=1}^s y_0^{d+1}g_1 \cdots g_s a_i(g_i t_i - f_i z) + z^d y_0^{d+1} \sum_{i=1}^n h_i(y_i^q - y_i) + z^d y_0^{d+1} G(y_1, \dots, y_n).$$

Thus to show that  $f \in I \cap S$  we need only show that  $G = 0$ . We claim that  $G$  vanishes on  $K^n$ . Notice that  $y_i^q - y_i$  vanishes at all points of  $K^n$  because  $(K^*, \cdot)$  is a group of order  $q - 1$ . Take an arbitrary sequence  $x_1, \dots, x_n$  of elements of  $K$ , i.e.,  $x = (x_i) \in K^n$ .

Case (I):  $g_i(x) = 0$  for some  $i$ . Making  $y_j = x_j$  for all  $j$  in Eq. (3.4) we get  $G(x) = 0$ .

Case (II):  $f_i(x) = 0$  and  $g_i(x) \neq 0$  for all  $i$ . Making  $y_k = x_k$  and  $t_j = f_j(x)/g_j(x)$  for all  $k, j$  in Eq. (3.4) and using that  $f$  is homogeneous, we obtain that  $G(x) = 0$ .

Case (III):  $f_i(x) \neq 0$  for some  $i$  and  $g_\ell(x) \neq 0$  for all  $\ell$ . Making  $y_k = x_k$ ,  $t_j = f_j(x)/g_j(x)$  and  $z = 1$  in Eq. (3.4) and using that  $f$  vanishes on  $[(f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))]$ , we get that  $G(x) = 0$ . This completes the proof of the claim.

Therefore  $G$  vanishes at all points of  $K^n$  and  $\deg_{y_i}(G) < q$  for all  $i$ . Hence, by Lemma 3.2, we get that  $G = 0$ .

Next we show the inclusion  $I(\mathbb{X}) \supset I \cap S$ . By Lemma 3.7 the ideal  $I \cap S$  is graded. Let  $f$  be a homogeneous polynomial of  $I \cap S$ . Take a point  $[P]$  in  $\mathbb{X}$  with  $P = (f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))$ . Writing  $f$  as a linear combination of  $\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1$ , with coefficients in  $K$ , and making  $t_i = f_i(x)/g_i(x)$ ,  $y_j = x_j$ ,  $z = 1$  and  $y_0 = 1/g_1(x) \cdots g_s(x)$  for all  $i, j$  it follows that  $f(P) = 0$ . Thus  $f$  vanishes on  $\mathbb{X}$ .  $\square$

**Definition 3.9.** If  $I \subset S$  is an ideal and  $h \in S$ , we set  $(I : h) := \{f \in S \mid fh \in I\}$ . This ideal is called the *colon ideal* of  $I$  with respect to  $h$ .

**Definition 3.10.** The *projective algebraic set parameterized by  $F$* , denoted by  $X$ , is the set of all points  $[(f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))]$  in  $\mathbb{P}^{s-1}$  such that  $x \in K^n$  and  $f_i(x)g_i(x) \neq 0$  for all  $i$ .

The ideal  $I(X)$  can be computed from  $I(\mathbb{X})$  using the colon operation.

**Proposition 3.11.** If  $X \neq \emptyset$ , then  $(I(\mathbb{X}) : t_1 \cdots t_s) = I(X)$ .

*Proof.* Since  $X \subset \mathbb{X}$ , one has  $I(\mathbb{X}) \subset I(X)$ . Consequently  $(I(\mathbb{X}) : t_1 \cdots t_s) \subset I(X)$  because  $t_i$  is not a zero-divisor of  $S/I(X)$  for all  $i$ . To show the reverse inclusion take a homogeneous polynomial  $f$  in  $I(X)$ . Let  $[P]$  be a point in  $\mathbb{X}$ , with  $P = (\alpha_1, \dots, \alpha_s)$  and  $\alpha_k \neq 0$  for some  $k$ , and let  $I_{[P]}$  be the ideal generated by the homogeneous polynomials of  $S$  that vanish at  $[P]$ . Then  $I_{[P]}$  is a prime ideal of height  $s - 1$ ,

$$(3.5) \quad I_{[P]} = (\{\alpha_k t_i - \alpha_i t_k \mid k \neq i \in \{1, \dots, s\}\}), \quad I(\mathbb{X}) = \bigcap_{[Q] \in \mathbb{X}} I_{[Q]},$$

and the latter is the primary decomposition of  $I(\mathbb{X})$ . Noticing that  $t_i \in I_{[P]}$  if and only if  $\alpha_i = 0$ , it follows that  $t_1 \cdots t_s f \in I(\mathbb{X})$ . Indeed if  $[P]$  has at least one entry equal to zero, then  $t_1 \cdots t_s \in I_{[P]}$  and if all entries of  $P$  are not zero, then  $f \in I(X) \subset I_{[P]}$ . In either case  $t_1 \cdots t_s f \in I(\mathbb{X})$ . Hence  $f \in (I(\mathbb{X}) : t_1 \cdots t_s)$ .  $\square$

Next we present some other means to compute the vanishing ideal  $I(X)$ .

**Theorem 3.12.** Let  $B = K[y_0, w, y_1, \dots, y_n, z, t_1, \dots, t_s]$  be a polynomial ring over  $K = \mathbb{F}_q$ . If  $X$  is a projective algebraic set parameterized by  $f_1/g_1, \dots, f_s/g_s$  in  $K(\mathbf{y})$  and  $X \neq \emptyset$ , then

$$\begin{aligned} I(X) &= (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1, w f_1 \cdots f_s - 1) \cap S \\ &= (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, \{f_i^{q-1} - 1\}_{i=1}^s, y_0 g_1 \cdots g_s - 1) \cap S. \end{aligned}$$

*Proof.* This follows adapting the proof of Theorem 3.8.  $\square$

**Theorem 3.13.** *Let  $B = K[y_0, y_1, \dots, y_n, t_1, \dots, t_s]$  be a polynomial ring over  $K = \mathbb{F}_q$ . If  $\mathbb{X}^*$  is an affine set parameterized by  $f_1/g_1, \dots, f_s/g_s$  in  $K(\mathbf{y})$ , then*

$$I(\mathbb{X}^*) = (\{g_i t_i - f_i\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S.$$

*Proof.* This follows adapting the proof of Theorem 3.8.  $\square$

**Definition 3.14.** The affine algebraic set parameterized by  $F$ , denoted  $X^*$ , is the set of all points  $(f_1(x)/g_1(x), \dots, f_s(x)/g_s(x))$  in  $\mathbb{A}^s$  such that  $x \in K^n$  and  $f_i(x)g_i(x) \neq 0$  for all  $i$ .

The ideal  $I(X^*)$  can be computed from  $I(\mathbb{X}^*)$  using the colon operation.

**Proposition 3.15.**  $(I(\mathbb{X}^*) : t_1 \cdots t_s) = I(X^*)$ .

*Proof.* This follows adapting the proof of Proposition 3.11.  $\square$

**Corollary 3.16.** *Let  $B = K[t_1, \dots, t_s, y_1, \dots, y_n, z]$  be a polynomial ring over the finite field  $K = \mathbb{F}_q$  and let  $f_1, \dots, f_s$  be polynomials of  $R$ . The following hold:*

- (a) *If  $\mathbb{X} \neq \emptyset$ , then  $I(\mathbb{X}) = (\{t_i - f_i z\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n) \cap S$ .*
- (b) *If  $X \neq \emptyset$ , then  $I(X) = (\{t_i - f_i z\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n \cup \{f_i^{q-1} - 1\}_{i=1}^s) \cap S$ .*

*Proof.* The result follows by adapting the proof of Theorem 3.8, and using Theorem 3.12.  $\square$

The formula for  $I(X)$  given in (b) can be slightly simplified if the  $f_i$ 's are Laurent monomials (see [11, Theorems 2.1 and 2.13]).

**Example 3.17.** Let  $f_1 = y_1 + 1$ ,  $f_2 = y_2 + 1$ ,  $f_3 = y_1 y_2$  and let  $K = \mathbb{F}_5$  be a field with 5 elements. Using Corollary 3.16, and *Macaulay2* [4], we get

$$\begin{aligned} \deg S/I(\mathbb{X}) &= 19, & \deg S/I(X) &= 6, \\ \text{reg } S/I(\mathbb{X}) &= 5, & \text{reg } S/I(X) &= 2. \end{aligned}$$

For convenience we present the following procedure for *Macaulay2* [4] that we used to compute the degree and the regularity:

```
R=GF(5)[z,y1,y2,t1,t2,t3,MonomialOrder=>Eliminate 3];
f1=y1+1,f2=y2+1,f3=y1*y2,q=5
I=ideal(t1-f1*z,t2-f2*z,t3-f3*z,y1^q-y1,y2^q-y2)
Jxx=ideal selectInSubring(1,gens gb I)
I=ideal(t1-f1*z,t2-f2*z,t3-f3*z,y1^q-y1,y2^q-y2,
f1^(q-1)-1,f2^(q-1)-1,f3^(q-1)-1)
Jx=ideal selectInSubring(1,gens gb I)
S=ZZ/5[t1,t2,t3]
Ixx=sub(Jxx,S),Mxx=coker gens Ixx
degree Ixx, regularity Mxx
Ix=sub(Jx,S),Mx=coker gens Ix
degree Ix, regularity Mx
```

**Example 3.18.** Let  $f_1 = y_1 + 1$ ,  $f_2 = y_2 + 1$ ,  $f_3 = y_1 y_2$  and let  $K = \mathbb{F}_5$  be a field with 5 elements. Using Proposition 2.7, Corollary 3.16 and *Macaulay2* [4], we get

$d$	1	2	3	4	5	$d$	1	2
$ \mathbb{X} $	19	19	19	19	19	$ X $	6	6
$\dim C_{\mathbb{X}}(d)$	3	6	10	15	19	$\dim C_X(d)$	3	6
$\delta_{\mathbb{X}}(d)$	13	8			1	$\delta_X(d)$	3	1

The  $d$ th column of these tables represent the length, the dimension, and the minimum distance of the projective Reed-Muller-type codes  $C_{\mathbb{X}}(d)$  and  $C_X(d)$ , respectively (see Section 2). The minimum distance was computed using the methods of [9]. Continuing with the *Macaulay2* procedure of Example 3.17 we can compute the other values of these two tables as follows:

```
degree Ixx, regularity Mxx
hilbertFunction(1,Ixx),hilbertFunction(2,Ixx),hilbertFunction(3,Ixx),
hilbertFunction(4,Ixx),hilbertFunction(5,Ixx)
degree Ix, regularity Mx
hilbertFunction(1,Ix),hilbertFunction(2,Ix)
```

Let us give some application to vanishing ideals over monomial parameterizations.

**Corollary 3.19.** *Let  $K = \mathbb{F}_q$  be a finite field. If  $\mathbb{X}$  is parameterized by Laurent monomials, then  $I(\mathbb{X})$  is a radical Cohen-Macaulay binomial ideal of dimension 1.*

*Proof.* That  $I(\mathbb{X})$  is a binomial ideal follows from Lemma 2.4 and applying Theorem 3.8. That  $I(\mathbb{X})$  is a radical ideal of dimension 1 is well known and follows from Eq. (3.5) (see the proof of Proposition 3.11). Recall that  $\text{depth } S/I(\mathbb{X}) \leq \dim S/I(\mathbb{X}) = 1$ . From Eq. (3.5) one has that  $\mathfrak{m} = (t_1, \dots, t_s)$  is not an associated prime of  $I(\mathbb{X})$ . Thus  $\text{depth } S/I(\mathbb{X}) > 0$  and  $\text{depth } S/I(\mathbb{X}) = \dim S/I(\mathbb{X}) = 1$ , i.e.,  $I(\mathbb{X})$  is Cohen-Macaulay.  $\square$

**Corollary 3.20.** [11, Theorem 2.1] *Let  $K = \mathbb{F}_q$  be a finite field and let  $X$  be a projective algebraic set parameterized by Laurent monomials. Then  $I(X)$  is a Cohen-Macaulay lattice ideal and  $\dim S/I(X) = 1$ .*

*Proof.* It follows from Proposition 3.11, Theorem 3.12 and Lemma 2.4.  $\square$

**Binomial vanishing ideals.** Let  $K$  be a field. The projective space  $\mathbb{P}^{s-1} \cup \{[0]\}$  together with the zero vector  $[0]$  is a monoid under componentwise multiplication, where  $[1] = [(1, \dots, 1)]$  is the identity of  $\mathbb{P}^{s-1} \cup \{[0]\}$ . Recall that monoids always have an identity element.

**Lemma 3.21.** *Let  $K = \mathbb{F}_q$  be a finite field and let  $\mathbb{Y}$  be a subset of  $\mathbb{P}^{s-1}$ . If  $\mathbb{Y} \cup \{[0]\}$  is a submonoid of  $\mathbb{P}^{s-1} \cup \{[0]\}$  such that each element of  $\mathbb{Y}$  is of the form  $[\alpha]$  with  $\alpha \in \{0, 1\}^s$ , then  $\mathbb{Y}$  is parameterized by Laurent monomials.*

*Proof.* The set  $\mathbb{Y}$  can be written as  $\mathbb{Y} = \{[\alpha_1], \dots, [\alpha_m]\}$ , where  $\alpha_i = (\alpha_{i1}, \dots, \alpha_{is})$  and  $\alpha_{ij} = 0$  or  $\alpha_{ik} = 1$  for all  $i, k$ . Consider variables  $y_1, \dots, y_s$  and  $z_1, \dots, z_s$ . For each  $\alpha_{ik}$  define  $h_{ik} = y_i^{q-1}$  if  $\alpha_{ik} = 1$  and  $h_{ik} = z_i^{q-1}/y_i^{q-1}$  if  $\alpha_{ik} = 0$ . Setting  $h_i = (h_{i1}, \dots, h_{is})$  for  $i = 1, \dots, m$  and  $F_i = h_{1i} \cdots h_{mi}$  for  $i = 1, \dots, s$ , we get

$$h_1 h_2 \cdots h_m = (h_{11} \cdots h_{m1}, \dots, h_{1s} \cdots h_{ms}) = (F_1, \dots, F_s).$$

It is not hard to see that  $\mathbb{Y}$  is parameterized by  $F_1, \dots, F_s$ .  $\square$



**Example 3.22.** Let  $K$  be the field  $\mathbb{F}_3$  and let  $\mathbb{Y} = \{[(1, 1, 0)], [0, 1, 1], [0, 1, 0], [1, 1, 1]\}$ . With the notation above, we get that  $\mathbb{Y}$  is the projective set parameterized by

$$F_1 = (y_1 z_2 z_3)^2 / (y_2 y_3)^2, F_2 = (y_1 y_2 y_3)^2, F_3 = (y_2 z_1 z_3)^2 / (y_1 y_3)^2.$$

The next result gives a family of ideals where the converse of Corollary 3.19 is true.

**Proposition 3.23.** *Let  $K = \mathbb{F}_q$  be a finite field. If  $\mathbb{Y}$  is a subset of  $\mathbb{P}^{s-1}$  such that each element of  $\mathbb{Y}$  is of the form  $[\alpha]$  with  $\alpha \in \{0, 1\}^s$  and  $I(\mathbb{Y})$  is a binomial ideal, then  $\mathbb{Y}$  is a projective set parameterized by Laurent monomials.*

*Proof.* Since  $\mathbb{Y}$  is finite, one has that  $\mathbb{Y} = \overline{\mathbb{Y}} = V(I(\mathbb{Y}))$ , where  $\overline{\mathbb{Y}}$  is the Zariski closure and  $V(I(\mathbb{Y}))$  is the zero set of  $I(\mathbb{Y})$ . Hence, as  $I(\mathbb{Y})$  is generated by binomials, we get that  $\mathbb{Y} \cup \{[0]\}$  is a submonoid of  $\mathbb{P}^{s-1} \cup \{[0]\}$ . Thus, by Lemma 3.21,  $\mathbb{Y}$  is parameterized by Laurent monomials.  $\square$

This leads us to pose the following conjecture.

**Conjecture 3.24.** Let  $K = \mathbb{F}_q$  be a finite field and let  $\mathbb{Y}$  be a subset of  $\mathbb{P}^{s-1}$ . If  $I(\mathbb{Y})$  is a binomial ideal, then  $\mathbb{Y}$  is a projective set parameterized by Laurent monomials.

In particular from Proposition 3.23 this conjecture is true for  $q = 2$ .

## REFERENCES

- [1] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Matraháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29. 3
- [2] D. Cox, J. Little and D. O’Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992. 1, 5
- [3] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, Finite Fields Appl. **8** (2002), no. 4, 511–518. 1, 2, 3
- [4] D. Grayson and M. Stillman, *Macaulay2*, 1996. Available via anonymous ftp from [math.uiuc.edu](http://math.uiuc.edu). 1, 7, 8
- [5] G. M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, 2nd extended edition, Springer, Berlin, 2008. 2
- [6] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992. 1
- [7] N. Jacobson, *Basic Algebra I*, Second Edition, W. H. Freeman and Company, New York, 1996. 2
- [8] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin, 2005. 1
- [9] J. Martínez-Bernal, Y. Pitones and R. H. Villarreal, Minimum distance functions of graded ideals and Reed-Muller-type codes, J. Pure Appl. Algebra, to appear. Preprint, 2015, arXiv:1512.06868v1. 8
- [10] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1986. 2
- [11] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl. **17** (2011), no. 1, 81–104. 1, 3, 7, 8
- [12] T. Sauer, Polynomial interpolation in several variables: lattices, differences, and ideals, Stud. Comput. Math. **12** (2006), 191–230. 1
- [13] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007. 1
- [14] R. H. Villarreal, *Monomial Algebras, Second Edition*, Monographs and Research Notes in Mathematics, Chapman and Hall/CRC, 2015. 2

DEPARTAMENTO DE MATEMÁTICAS, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN, APARTADO POSTAL 14–740, 07000 MEXICO CITY, D.F.

*E-mail address:* [tochimani@math.cinvestav.mx](mailto:tochimani@math.cinvestav.mx)

DEPARTAMENTO DE MATEMÁTICAS, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN, APARTADO POSTAL 14–740, 07000 MEXICO CITY, D.F.

*E-mail address:* [vila@math.cinvestav.mx](mailto:vila@math.cinvestav.mx)